

A

Paper 1

Filed by: Jameson Lee
Administrative Patent Judge
Mail Stop Interference
P.O. Box 1450
Alexandria Va 22313-1450
Tel: 703-308-9797
Fax: 703-305-0942

Filed
4 September 2003

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

GREG BENSON, GREGORY H. URICH
and CHRISTOPHER L. KNAUFT,
Junior Party,
(Patent 5,845,281; Applications 09/164,606
and 09/321,386),

v.

KARL L. GINTER, VICTOR H. SHEAR,
FRANCES J. SPAHN and DAVID M. VAN WIE,
Senior Party,
(Application 09/411,205).

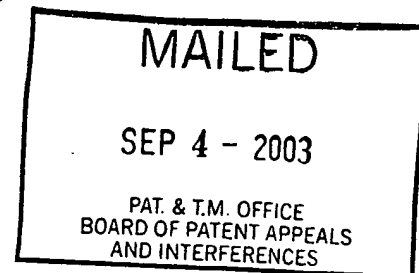
Patent Interference No. 105,142

NOTICE DECLARING INTERFERENCE
(37 CFR § 1.611)

Part A. Declaration of interference

An interference is declared (35 U.S.C. § 135(a)) between the above-identified parties.

Details of the application(s), patent (if any), reissue application (if any), count(s) and claims designated as corresponding or as not corresponding to the count(s) appear in Parts E and F of this NOTICE DECLARING INTERFERENCE.



RECEIVED

MAR 08 2004

Technology Center 2100

Part B. Judge designated to handle the interference

Administrative Patent Judge Jameson Lee has been designated to handle the interference.

37 CFR § 1.610(a).

Part C. Standing order

A Trial Section STANDING ORDER accompanies this NOTICE DECLARING INTERFERENCE. The STANDING ORDER applies to this interference.

Part D. Conference call to set dates

A telephone conference call to set dates for taking action in the interference is scheduled for **2:00 p.m. on 21 October 2003** (the call will be initiated from the PTO).

No later than **two business days** prior to the conference call, each party shall file and serve by facsimile a list of the preliminary motions the party intends to file. See STANDING ORDER ¶ 10.

A copy of a "sample" order setting times for taking action during the preliminary motion phase of the interference, accompanies this NOTICE DECLARING INTERFERENCE. Counsel are encouraged to discuss the order prior to the conference call with the view to coming to some agreement as to dates for taking action. A typical preliminary motion period lasts approximately nine (9) months. Counsel should be prepared to justify any request for a shorter or longer period.

Part E. The parties involved in this interference are:

Junior Party

Named inventor: GREG BENSON, Dalby, Sweden
GREGORY H. URICH, Lund, Sweden
CHRISTOPHER L. KNAUFT, San Diego, CA

Patent: 5,845,281, granted 1 December 1998, based on
application 08/594,811, filed 31 January 1996

Title: Method and system for managing a data object
so as to comply with predetermined conditions
for usage

Assignee: Greg Benson

Accorded Benefit: none

Attorneys: See last page

Address: See last page

Application: 09/164,606, filed 1 October 1998

Title: Method and system for managing a data object
so as to comply with predetermined conditions
for usage

Assignee: Macrovision Corporation

Accorded Benefit: Patent 5,845,281, granted 1 December 1998, based
on application 08/594,811, filed 31 January 1996

Attorneys: See last page

Address: See last page

Application: 09/321,386, filed 27 May 1999

Title: Method and system for managing a data object
so as to comply with predetermined conditions
for usage

Assignee: Macrovision Corporation

Accorded Benefit: Patent 5,845,281, granted 1 December 1998, based on application 08/594,811, filed 31 January 1996; Application 09/164,606, filed 1 October 1998

Attorneys: See last page

Address: See last page

Senior Party

Named Inventor: KARL L. GINTER, Beltsville, MD
VICTOR H. SHEAR, Bethesda, MD
FRANCIS J. SPAHN, El Cerrito, CA
DAVID M. VAN WIE, Sunnyvale, CA

Application: 09/411,205, filed 4 October 1999

Title: System and methods for secure transaction management and electronic rights protection

Assignee: none

Accorded Benefit: Patent 6,253,193, granted 26 June 2001, based on application 09/208,017, filed 9 December 1998; Patent 5,982,891, granted 9 November 1999, based on application 08/964,333, filed 4 November 1997; Application 08/388,107, filed 13 February 1995

Attorneys: See last page

Address: See last page

Part F. Count and claims of the parties

Count 1

Claim 1 of Benson's Application 09/321,386 (Benson III)

The claims of the parties corresponding to Count 1 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 1-3, 5-12, 15-19 and 22-29
Ginter's Application 09/411,205:	Claims 91-93, 95-102, 105-109, 112-119, 120-122, 124-131, 134-138 and 141-148
Benson's Application 09/164,606 (Benson II):	Claims 30-32, 34-41, 44-46, 48, 51, 56, 58-66, 68 and 69
Benson's Application 09/321,386 (Benson III):	Claims 1-3, 5-12, 15-17, 19, 22, 27, 29-37 and 39-53

The claims of the parties **not** corresponding to Count 1 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 4, 13, 14, 20 and 21
Ginter's Application 09/411,205:	Claims 94, 103, 104, 110, 111, 123, 132, 133, 139 and 140
Benson's Application 09/164,606 (Benson II):	Claims 33, 42, 43, 47, 49, 50, 52-55, 57 and 67
Benson's Application 09/321, 386 (Benson III):	Claims 4, 13, 14, 18, 20, 21, 23-26, 28 and 38

Count 2

Claim 4 of Benson's Application 09/321,386 (Benson III)

The claims of the parties corresponding to Count 2 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 4, 13 and 14
Ginter's Application 09/411,205:	Claims 94, 103, 104, 123, 132 and 133
Benson's Application 09/164,606 (Benson II):	Claims 33, 42, 43, 47, 49, 50, 57 and 67
Benson's Application 09/321, 386 (Benson III):	Claims 4, 13, 14, 18, 20, 21, 28 and 38

The claims of the parties **not** corresponding to Count 2 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 1-3, 5-12 and 15-29
Ginter's Application 09/411,205:	Claims 91-93, 95-102, 105-122, 124-131 and 134-148
Benson's Application 09/164,606 (Benson II):	Claims 30-32, 34-41, 44-46, 48, 51-56, 58-66, 68 and 69
Benson's Application 09/321, 386 (Benson III):	Claims 1-3, 5-12, 15-17, 19, 22-27, 29-37 and 39-53

Count 3

Claim 23 of Benson's Application 09/321,386 (Benson III)

The claims of parties corresponding to Count 3 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 20 and 21
Ginter's Application 09/411,205:	Claims 110, 111, 139 and 140
Benson's Application 09/164,606 (Benson II):	Claims 52, 53 and 55
Benson's Application 09/321,386 (Benson III):	Claims 23 and 24

The claims of the parties **not** corresponding to Count 3 are:

Benson's Patent No. 5,845,281 (Benson I):	Claims 1-19 and 22-29
Ginter's Application 09/411,205:	Claims 91-109, 112-138 and 141-148
Benson's Application 09/164,606 (Benson II):	Claims 30-51, 54 and 56-69
Benson's Application 09/321, 386 (Benson III):	Claims 1-22 and 25-53

Part G. Heading to be used on papers

The following heading shall be used on papers filed in the interference. See **STANDING**

ORDER ¶ 3.5.

Paper ____¹

Filed on behalf of [name of party]

By: Name of lead counsel
Name of backup counsel
Street address
City, State, and Zip-Code
Tel:
Fax:

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES
(Administrative Patent Judge Jameson Lee)

GREG BENSON, GREGORY H. URICH
and CHRISTOPHER L. KNAUFT,
Junior Party,
(Patent 5,845,281; Applications 09/164,606
and 09/321,386),

v.

KARL L. GINTER, VICTOR H. SHEAR,
FRANCES J. SPAHN and DAVID M. VAN WIE,
Senior Party,
(Application 09/411,205).

Patent Interference No. 105,142

TITLE OF PAPER

¹ Leave a blank line because the board assigns the paper number.

Part H. Summary of dates for taking action

Times for taking action are set out in the following sections of the STANDING ORDER:

- ¶ 4: date for identifying lead and backup counsel.
- ¶ 5: date for identifying any real party in interest.
- ¶ 6: date for requesting copies of involved and benefit applications and patents.
- ¶ 7: date for accomplishing certain discovery.
- ¶ 8: date for filing clean copy of claims.
- ¶ 9: date for filing clean copy of claims in cases with drawings or claims containing a means plus function limitation.
- ¶ 10: date for filing list of proposed preliminary motions.
- ¶ 13.10.2: dates for filing oppositions to Rule 635 miscellaneous motions and dates for filing replies to oppositions.
- ¶ 14.1.1: date for objecting to admissibility of evidence.
- ¶ 14.2: date for serving supplemental affidavits or evidence to respond to objection to admissibility of evidence.
- ¶ 14.3: dates when cross-examination can take place.
- ¶ 15.2: dates for taking action with respect to settlement discussions.

Part I. Order form for requesting file copies

FILE COPY REQUEST
Interference 105,142

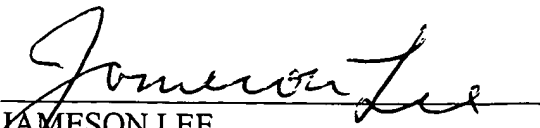
A copy of Part E of this NOTICE DECLARING INTERFERENCE should be attached to this FILE COPY REQUEST, with a circle by hand around the patents and applications for which a copy of a file wrapper is desired.

To facilitate processing of this FILE COPY REQUEST, the following information should be included:

1. Charge fees to USPTO Deposit Account No. _____
2. Complete address, including street, city, state, ZIP code and telephone number (do not list a Post Office box because file copies are sent via commercial overnight courier).

Telephone, including area code: _____

Part J. Signature of administrative patent judge


JAMESON LEE
Administrative Patent Judge

Date: 9/4/03

Enc:

Copy of STANDING ORDER

Copy of order used for setting times for taking action in the preliminary motion phase of the interference

Copy of order used for setting times for taking action in the testimony and briefing phases of the interference

Copy of Patent No. 5,845,281 (Benson I)

Copy of claims of Serial No. 09/411,205

Copy of claims of Serial No. 09/164,606 (Benson II)

Copy of claims of Serial No. 09/321,386 (Benson III)

Revised May 2003

cc (via Federal Express):

Attorney for BENSON:

Frank Nguyen
MACROVISION CORPORATION
2830 De La Cruz Boulevard
Santa Clara, CA 95050

Attorney for GINTER:

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
1301 I Street, N.W.
Washington, D.C. 20005

MEDIDNA.001C1

#2
Re And A
PATENT C

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Benson et al.) Group Art Unit Unassigned
Appl. No. : Unassigned 09/164,606)
Filed : Herewith)
For : METHOD AND SYSTEM FOR)
MANAGING A DATA)
OBJECT SO AS TO COMPLY)
WITH PREDETERMINED)
CONDITIONS FOR USAGE)
Examiner : Unassigned)

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Prior to an examination on the merits, please enter the amendments below.

IN THE CLAIMS:

Please cancel Claims 1-29, without disclaimer or prejudice.

Please add the following new Claims 30-69 as follows:

30. A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

providing a variable number of control conditions for usage of the data object;
providing a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions;

combining the general set of control data with the data object; and

Appl. No. : Unass^d
Filed : Herewith

encrypting the data object and the one or more usage control elements to create a secure data package.

2 31. The method of Claim 30¹, additionally comprising encrypting together the data object and the general set of control data.

3 32. The method of Claim 30¹, wherein providing the general set of control data includes providing an identifier which uniquely identifies the general set of control data.

4 33. The method of Claim 30¹, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

5 34. The method of Claim 30¹, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

6 35. The method of Claim 30¹, additionally comprising:
receiving a request for authorization for usage by a user;
comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and
granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

7 36. The method of Claim 35⁶, additionally comprising requiring payment for the requested authorization for usage before granting the authorization.

8 37. The method of Claim 30¹, additionally comprising:
transmitting the secure data package into a data processor;

Appl. No. : Unpublished
Filed : Herewith

checking, in response to a request by a user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object so as to enable the requested usage.

- 9 ⁸
38. The method of Claim 37, additionally comprising:
combining, after the usage of the data object, the data object and the one or more usage control elements; and
reencrypting at least the data object and the one or more usage control elements.

- 10
39. A method of controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:
providing a variable number of control conditions for usage of the data object;
providing a data package comprising a data object and control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of control conditions, the data object and the at least one usage control element being encrypted;
receiving a request by the user for usage of the data object;
decrypting the control data;
checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and
decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage.

- 11
40. The method of Claim 39, wherein the usage control element is updated after the at least one usage of the data object.

Appl. No. : Unas. ~~rd~~
Filed : Herewith

¹²41. The method of Claim ¹⁰39, wherein the control data comprises an indication of the number of times the user is authorized to use the data object in accordance with the at least one usage control element, wherein the requested usage of the data object is only enabled when the number of times is one or more, and wherein the number of times is decremented by one when the requested usage is enabled.

¹³42. The method of Claim ¹⁰39, wherein the control data comprise a security control element, and additionally comprising executing, before each usage of the data object, a security procedure defined in the security control element.

¹⁴43. The method of Claim ¹⁰39, wherein checking whether the requested usage complies with the usage defined by the at least one usage control element, comprises checking that a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

¹⁵44. The method of Claim ¹⁰39, additionally comprising:
combining, after the usage of the data object, the data object and the one or more usage control elements; and
reencrypting at least the data object and the one or more usage control elements.

¹⁶45. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

- a user interface module which receives a variable number of control conditions;
- a packaging module which provides a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions and which combines the general set of control data with the data object; and

Appl. No. : Unpublished
Filed : Herewith

an encrypting module which encrypts the data object and at least the one or more usage control elements to create a secure data package necessary.

¹⁷
46. The system of Claim ¹⁶45, wherein the general set of control data comprises a control data element which controls further distribution of the data object.

¹⁸
47. The system of Claim ¹⁶45, wherein one of the usage control elements includes a security control element that defines a security procedure.

¹⁹
48. The system for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

a usage manager module which receives a variable number of control conditions, checks whether a usage requested by the user complies with the usage defined by at least one usage control element that complies with the variable number of control conditions, and disables the usage requested by the user when the usage does not comply with the usage defined by the at least one usage control element; and

a decryption module which decrypts the at least one usage control element and the data object.

²⁰
49. The system of Claim ¹⁹48, wherein one of the usage control elements includes a security control element that defines a security procedure.

²¹
50. The system of Claim ²⁰49, wherein the security procedure is an RSA encryption algorithm.

²²
51. The system of Claim ¹⁹48, wherein the usage manager module repackages the data object after usage.

²³
52. A method of controlling the usage by a user of data objects so as to comply with a variable number of conditions for usage of the data objects, comprising:

Appl. No. : Unpublished
Filed : Herewith

providing at least two data packages, each data package comprising a data object and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of conditions, the data object and the at least one usage control elements being encrypted;

decrypting the usage control elements of the user sets of control data;

examining the usage control elements of the at least two data packages to find a match; and

performing an action being specified in the user sets of control data of the at least two data packages.

²⁴53. The method of Claim ²³52, wherein one of the at least two data packages is a sell order, and wherein one of the at least two data packages is a buy order.

²⁵54. The method of Claim ²³52, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure.

²⁶55. The method of Claim ²³52, additionally comprising:
updating the at least one usage control element of each data package;
combining after the usage of the data objects, each of the data objects and its at least one usage control element;
reencrypting each of the combined data objects and its at least one usage control element; and
transferring the repackaged data objects to their providers.

²⁷56. A method of managing a data object so as to comply with a variable number of control conditions for usage of the data object, comprising:
providing variable control conditions for usage of the data object;

Appl. No. : Unassigned
Filed : Herewith

providing a general set of control data for the data object based on the variable control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable control conditions;

providing, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of the usage control elements;

combining the user set of control data with the data object;

encrypting at least the data object and the at least one of the usage control elements of the user set of control data to create a secure data package; and

checking, before allowing transfer of the data package to the user, that the request for authorization for usage of the data object has been granted.

26
57. The method of Claim 27²⁷, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure.

29
58. The method of Claim 27²⁷, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of the constituent data objects by a user, is created only for that constituent data object and combined only with a copy of that constituent data object.

30
59. The method of Claim 27²⁷, wherein the request for authorization is received from a user via a data network.

31
60. The method of Claim 27²⁷, wherein the data object is a composite data object including at least two constituent data objects, and wherein providing a general set of control data comprises providing a respective general set of control data for each of the constituent data objects and the composite data object, and wherein providing a user set of control data comprises

Appl. No. : Unpublished
Filed : Herewith

providing a respective user set of control data for each of the constituent data objects and the composite data object.

³²61. The method as defined in Claim ²⁷56, additionally comprising storing the user set of control data in a processor of a data object provider.

³³62. The method as defined in Claim ²⁷56, additionally comprising:
transmitting the data package;
decrypting the at least one usage control element of the user set of control data;
checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and
decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage.

³⁴63. The method of Claim ²⁷56, additionally comprising:
transmitting the data package;
decrypting the at least one usage control element of the user set of control data;
checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data;
decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage; and
combining, after the usage of the data object, the data object and the one or more usage control elements of the user set of control data, and combining at least the data object and the one or more usage of the user set of control data.

³⁵64. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

Appl. No. : Unpublished
Filed : Herewith

a packaging module which provides a general set of control data for the data object based on variable conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable conditions and which combines the user set of control data with the data object, and wherein the packaging module provides in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of the usage control elements;

an encrypting module which encrypts the data object and at least the one or more usage control elements of the user set of control data to create a secure data package, which is ready for transfer to a user; and

a control module which checks that the request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

36
65. A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

providing a general set of control data for the data object based on a variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions; and

encrypting the data object and the one or more usage control elements to create at least one secure data package.

37
66. The method of Claim 36, wherein the data object and the usage control elements are each encrypted into separate secure packages.

38
67. The method of Claim 36, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

Appl. No. : Unpublished
Filed : Herewith

³⁹ 68. The method of Claim ³⁶ 65, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

⁴⁰ 69. The method of Claim ³⁶ 65, additionally comprising:
receiving a request for authorization for usage by a user;
comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and
granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 10/1/98

By: _____

John M. Carson
Registration No. 34,303
Attorney of Record
620 Newport Center Drive
Sixteenth Floor
Newport Beach, CA 92660
(619) 235-8550

S:\DOCS\EMN\EMN-1526.DOC/kz9
060198

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Greg Benson; Gregory H. Urich; Christopher L. Knauff
Assignee: Macrovision Corporation
Title: METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO
AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR
USAGE
Serial No.: 09/321,386 Filing Date: May 27, 1999
Examiner: M. Von Buhr Group Art Unit: 2171
Docket No.: M-15081 US

24/9
CBanner
8/22/03

Mail Stop Amendment
COMMISSIONER FOR PATENTS
Arlington, VA 22313-1450

Irvine, California
August 22, 2003

AMENDMENT

Dear Sir:

Applicants submit the following amendments and remarks.

LAW OFFICES OF
MACPHERSON KWOK
CHEN & BYRD LLP

2402 MICHELSON DR.
SUITE 210
IRVINE, CA 92613
(949) 752-7040
FAX (949) 752-7049

v.1

IN THE CLAIMS

Please cancel Claims 55-63, 67-74, 77-78, 81-82, 86-87, and 96-150.

1. (original) A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

storing a data object in the memory of a data object provider processor;
providing a variable number of control conditions for usage of the data object;
providing a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions; and

encrypting at least the data object to create a secure data package so that it is ready to transfer to a user data processor.

2. (original) The method of Claim 1, additionally comprising encrypting together the data object and the general set of control data.

3. (original) The method of Claim 1, wherein providing the general set of control data includes providing an identifier which uniquely identifies the general set of control data.

4. (original) The method of Claim 1, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

5. (original) The method of Claim 1, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

6. (original) The method of Claim 1, additionally comprising:
receiving a request for authorization for usage by a user;
comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and

granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

7. (original) The method of Claim 6, additionally comprising requiring payment for the requested authorization for usage before granting the authorization.

8. (original) The method of Claim 1, additionally comprising:
transmitting the secure data package into the data processor;
checking, in response to a request by a user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data; and
decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object so as to enable the requested usage.

9. (original) The method of Claim 8, additionally comprising:
combining, after the usage of the data object, the data object and the one or more usage control elements; and
reencrypting at least the data object.

10. (original) A method of controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

providing a variable number of control conditions for usage of the data object;
providing a data object and control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of control conditions, the data object being encrypted;

receiving a request by the user for usage of the data object;

checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage.

11. (original) The method of Claim 10, wherein the usage control element is updated after the at least one usage of the data object.

12. (original) The method of Claim 10, wherein the control data comprises an indication of the number of times the user is authorized to use the data object in accordance with the at least one usage control element, wherein the requested usage of the data object is only enabled when the number of times is one or more, and wherein the number of times is decremented by one when the requested usage is enabled.

13. (original) The method of Claim 10, wherein the control data comprise a security control element, and additionally comprising executing, before each usage of the data object, a security procedure defined in the security control element.

14. (original) The method of Claim 10, wherein checking whether the requested usage complies with the usage defined by the at least one usage control element, comprises checking that a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

15. (original) The method of Claim 10, additionally comprising:
 combining, after the usage of the data object, the data object and the one or more usage control elements; and
 reencrypting at least the data object.

16. (original) A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

a user interface module which receives a variable number of control conditions;

a packaging module which provides a general set of control data for the data object based on the variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of

the data object which comply with the variable number of control conditions and which packages the general set of control data; and

an encrypting module which encrypts the data object to create a secure data package, which is ready for transfer to a user.

17. (original) The system of Claim 16, wherein the general set of control data comprises a control data element which controls further distribution of the data object.

18. (original) The system of Claim 16, wherein one of the usage control elements includes a security control element that defines a security procedure.

19. (original) A system for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

a usage manager module which receives a variable number of control conditions, checks whether a usage requested by the user complies with the usage defined by at least one usage control element that complies with the variable number of control conditions, and disables the usage requested by the user when the usage does not comply with the usage defined by the at least one usage control element; and
a decryption module which decrypts the data object, responsive to the check for requested usage by the usage manager module.

20. (original) The system of Claim 19, wherein one of the usage control elements includes a security control element that defines a security procedure.

21. (original) The system of Claim 20, wherein the security procedure is an RSA encryption algorithm.

22. (original) The system of Claim 19, wherein the usage manager module encrypts the data object after usage.

23. (original) A method of controlling the usage by a user of data objects so as to comply with a variable number of conditions for usage of the data objects, comprising:

providing at least two data packages, each data package comprising a data object and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of conditions, the data object being encrypted;

examining the usage control elements of the at least two data packages to find a match; and

performing an action being specified in the user sets of control data of the at least two data packages.

24. (original) The method of Claim 23, wherein one of the at least two data packages is a sell order, and wherein one of the at least two data packages is a buy order.

25. (original) The method of Claim 23, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure, and decrypting the data objects.

26. (original) The method of Claim 25, additionally comprising:
updating the at least one usage control element of each data package; and
reencrypting each of the data object.

27. (original) A method of managing a data object so as to comply with a variable number of control conditions for usage of the data object, comprising:

providing variable control conditions for usage of the data object;

providing a general set of control data for the data object based on the variable control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable control conditions;

providing, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of the usage control elements;

encrypting at least the data object to create a secure data package; and

checking, before allowing transfer of the data package to the user, that the request for authorization for usage of the data object has been granted.

28. (original) The method of Claim 27, additionally comprising checking whether a data processor is capable of executing a security procedure specified in a security control element of the at least one usage control element, and disabling the usage when the data processor is not capable of executing the security procedure.

29. (original) The method of Claim 27, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of the constituent data objects by a user, is created only for that constituent data object and combined only with a copy of that constituent data object.

30. (original) The method of Claim 27, wherein the request for authorization is received from a user via a data network.

31. (original) The method of Claim 27, wherein the data object is a composite data object including at least two constituent data objects, and wherein providing a general set of control data comprises providing a respective general set of control data for each of the constituent data objects and the composite data object, and wherein providing a user set of control data comprises providing a respective user set of control data for each of the constituent data objects and the composite data object.

32. (original) The method as defined in Claim 27, additionally comprising storing the user set of control data in a processor of a data object provider.

33. (original) The method as defined in Claim 27, additionally comprising:
transmitting the data package;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage.

34. (original) The method of Claim 27, additionally comprising:
transmitting the data package; and
reencrypting the data object.

35. (original) A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

a packaging module which provides a general set of control data for the data object based on variable conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable conditions and which combines the user set of control data with the data object, and wherein the packaging module provides in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of the usage control elements;

an encrypting module which encrypts the data object to create a secure data package, which is ready for transfer to a user; and

a control module which checks that the request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

36. (original) A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

providing a general set of control data for the data object based on a variable number of control conditions for usage, the general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions; and

encrypting at least the data object to create at least one secure data package, which is ready for transfer to a user.

37. (original) The method of Claim 36, wherein the data object and the usage control elements are encrypted into a single secure package.

38. (original) The method of Claim 36, wherein providing the general set of control data includes providing a security control element which identifies a security process to be applied before usage of the data object is allowed.

39. (original) The method of Claim 36, wherein providing the general set of control data includes providing a format control element which identifies the format of the control data.

40. (original) The method of Claim 36, additionally comprising:
 receiving a request for authorization for usage by a user;
 comparing the usage for which authorization is requested with the one or more usage control elements of the general set of control data; and
 granting the authorization if the usage for which authorization is requested complies with the usages defined by the one or more usage control elements.

41. (original) A method of managing a data object at a data provider computer so as to comply with control conditions for usage of the data object, comprising:
 providing a variable set of control data for the data object, the variable set of control data including usage information regarding the data object;
 concatenating the variable set of control data with the data object; and
 encrypting at least the data object to create at least one secure data package that is ready for transmission to a user data processor.

42. (original) The method of Claim 41, wherein the encrypting includes storing the at least one secure data package at the data provider computer.

43. (original) A method of managing a data object at a data provider computer so as to comply with control conditions for usage of the data object, comprising:

providing a set of control data for the data object based on a variable number of control conditions for usage, the set of control data including usage information regarding the data object;

combining the set of control data with the data object; and

encrypting at least the data object to create at least one secure data package, so that the at least one secure data package is stored in the data provider computer.

44. (original) The method of Claim 43, additionally comprising transmitting the at least one secure data package to the user data processor.

45. (original) The method of Claim 43, wherein the data object comprises digital money.

46. (original) The method of Claim 43, wherein the data object comprises an empty file.

47. (original) The method of Claim 43, wherein the data object is created by an author.

48. (original) A method of managing a data object so as to comply with control conditions for usage of the data object, comprising:

storing a data object in the memory of a data object provider processor;

providing a variable number of control conditions for usage of the data object;

and

providing a set of control data for the data object based on the variable number of control conditions for usage, the set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions.

49. (original) The method of Claim 48, additionally comprising:
transmitting the data object and the set of control data into a data processor;
and

checking, in response to a request by a user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the set of control data; and

complying with the usage defined by the at least one usage control element of the set of control data so as to enable the requested usage.

91 50. (original) The method of Claim 49, additionally comprising combining, after the usage of the data object, the data object and the one or more usage control elements.

51. (original) The method of Claim 49, wherein the data object comprises digital data.

52. (original) The data object of Claim 49, wherein the control data comprises an object identifier.

53. (original) The data object of Claim 49, wherein the data object comprises a video file.

54. (previously canceled)

55. - 63. (canceled)

64. - 66. (previously canceled)

67. - 74. (canceled)

75. - 76. (previously canceled)

77. - 78. (canceled)

79. - 80. (previously canceled)

81. - 82. (canceled)

Copy for Administrative Patent Judge

Patent 2/5/01
Attorney's Docket No. 032406-002
#5C
1W
(A/E)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)

Karl L. GINTER, et al.)

Application No.: 09/411,205)

Filed: October 4, 1999)

For: SYSTEMS AND METHODS FOR)
SECURE TRANSACTION)
MANAGEMENT AND ELECTRONIC)
RIGHTS PROTECTION)

Group Art Unit: 2171

Examiner: Von Buhr, M.

RECEIVED

JAN 26 2001

Technology Center 2100

AMENDMENT AND REQUEST FOR INTERFERENCE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In response to the Office Action dated December 19, 2000, please amend the above-identified application as follows:

IN THE SPECIFICATION:

On page 1, before the heading "Field(s) of the Invention(s)," insert the following paragraph:

sub
DV
01
This application is a continuation of Application No. 09/208,017 filed December 9, 1999, which is a continuation of Application No. 08/388,107 filed February 13, 1995, now abandoned.

IN THE CLAIMS:

Please cancel claims 1-90 of the application as originally filed and add new claims 91-148 as follows:

- 91. A method for managing a data object so as to comply with control conditions for usage of the data object, comprising the steps of:
- storing the data object in a memory device, where it is accessible by means of a data object provider's data processor;
 - providing a variable number of control conditions for usage of the data object;
 - creating, by said data processor, a general set of control data for the data object based on said variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with said variable number of control conditions,
 - storing said general set of control data in a memory device, where it is accessible by said data processor;
 - concatenating the general set of control data with a copy of the data object; and
 - encrypting at least the copy of the data object and said one or more usage control elements to create a secure data package which is ready for transfer to a user.
92. A method as set forth in claim 91, wherein the step of encrypting comprises encrypting the data object and the general set of control data.

93. A method as set forth in claim 91, wherein the step of creating control data comprises creating an identifier which uniquely identifies the general set of control data.

94. A method as set forth in claim 91, wherein the step of creating a general set of control data comprises creating a security control element which identifies a security process to be applied before usage of the data object is allowed.

95. A method as set forth in claim 91, wherein the step of creating a general set of control data comprises creating a format control element which identifies the format of the control data.

96. A method as set forth in claim 91, further comprising the steps of receiving in said data processor a request for authorization for usage by a user; comparing the usage for which authorization is requested with said one or more usage control elements of the general set of control data and granting the authorization if the usage for which authorization is requested complies with the usages defined by said one or more usage control elements.

97. A method as set forth in claim 96, further comprising the step of securing payment for the requested authorization for usage before granting the authorization.

98. A method as set forth in claim 91, comprising the further steps of:

- receiving the data package in a user's data processor;
- storing the data package in a memory device where it is accessible by means of the user's data processor;
- decrypting said one or more usage control elements;
- checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data;
- decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object and enabling the requested usage, otherwise disabling it.

99. A method as set forth in claim 98, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

100. A method for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising the steps of:

- providing a variable number of control conditions for usage of the data object;

storing a data package in a memory device, where it is accessible by means of a data processor of the user, said data package comprising the data object and control data, which comprises at least one usage control element defining a usage of the data object which complies with the variable number of control conditions, the data object and said at least one usage control element being encrypted;

receiving a request by the user for usage of the data object;

decrypting the control data;

checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage, otherwise disabling it.

101. A method as set forth in claim 100, wherein the usage control element is updated after the at least one usage of the data object.

102. A method as set forth in claim 100, wherein said control data comprises an indication of the number of times the user is authorized to use the data object in accordance with said at least one usage control element;

wherein the requested usage of the data object is only enabled when said number of times is one or more; and

wherein said number of times is decremented by one when the requested usage is enabled.

103. A method as set forth in claim 100, wherein the control data comprise a security control element, and further comprising the step of carrying out, before each usage of the data object, a security procedure defined in the security control element.

104. A method as set forth in claim 100, wherein the step of checking whether the requested usage complies with the usage defined by the at least one usage control element comprises the step of checking that the user's data processor is capable of carrying out a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

105. A method as set forth in claim 100, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

106. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising means for providing a variable number of control conditions;

first means in the data object provider's data processor for creating a general set of control data for the data object based on the variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the variable number of control conditions;

storing means, which are accessible by means of said data processor, for storing the data object and the general set of control data;

concatenating means for concatenating the general set of control data with a copy of the data object; and

encrypting means for encrypting the copy of the data object and at least said one or more usage control elements to create a secure data package, which is ready for transfer to a user.

107. A system as set forth in claim 106, wherein the general set of control data comprises a control data element which defines the right to further distribution of the data object by the user.

108. A system for controlling the usage by a user of a data object so as to comply with control conditions for usage of the data object, comprising:

means for providing variable number of control conditions;

storing means for storing a data package which comprises a data object and a control data comprising at least one usage control element defying a usage of the data object which complies with the variable number of control conditions;

means for decrypting the at least one usage control element and the data object;

checking means for checking whether a usage requested by the user complies with the usage defined by said at least one usage control element;

enabling means for enabling the usage requested by the user when the usage complies with the usage defined by said at least one usage control element; and

disabling means for disabling the usage requested by the user when the usage does not comply with the usage defined by said at least one usage control element.

109. A system as set forth in claim 108, further comprising means for repackaging the data object after usage thereof.

110. A method for controlling the usage by a user of data objects so as to comply with predetermined conditions for usage of the data objects, comprising the steps of:

storing at least two data packages in a memory device, where they are accessible by a data processor of the user, each said data package comprising a data object and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the predetermined conditions, the data object and said at least one usage control elements being encrypted;

decrypting the usage control elements of the user sets of control data;

examining the usage control elements of said at least two data packages to find a match;

using, in response to the finding of a match, the data processor to carry out an action, which is specified in the user sets of control data.

111. A method as set forth in claim 110, comprising the further steps of updating the at least one usage control element of each data package, concatenating after the usage of the data objects, each of the data objects and its at least one usage control element, reencrypting each of the concatenated data objects and its at least one usage control element and transferring the repackaged data objects to their creators.

112. A method for managing a data object so as to comply with predetermined conditions for usage of the data object, comprising the steps of:

storing the data object in a memory device, where it is accessible by means of a data object provider's data processor;

providing control conditions for usage of the data object;

creating, by said data processor, a general set of control data for the data object based on said control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with said control conditions;

storing said general set of control data in a memory device, where it is accessible by said data processor;

concatenating the general set of control data with a copy of the data object;

encrypting at least the copy of the data object and said one or more usage control elements to create a secure data package which is ready for transfer to a user;

creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of said usage control elements;

using the user set of control data instead of the general set of control data in said concatenating step;

using the at least one or more usage control element of the user set of control data instead of the one or more usage control elements of the general set of control data in the encrypting step; and

checking, before allowing transfer of the data package to the user, that said request for authorization for usage of the data object has been granted.

113. A method as set forth in claim 112, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent data objects by a user, is created only for that constituent data object and concatenated only with a copy of that constituent data object.

114. A method as set forth in claim 112, wherein the data provider's data processor is connected to a data network and the request for authorization is received from a data processor of the user, which is also connected to the data network, further comprising the step of transferring the data package through the data network to the user's data processor.

115. A method as set forth in claim 112, wherein the data object is a composite data object including at least two constituent data objects and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent data objects and the composite data object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent data objects and the composite data object.

116. A method as defined in claim 112, comprising the further step of storing a copy of the user set of control data in the data object provider's processor.

117. A method as defined in claim 112, comprising the further steps of:

receiving the data package in a user's data processor;

storing the data package in a memory device where it is accessible by means of the user's data processor;

decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage, otherwise disabling it.

118. A method as set forth in claim 112, further comprising:

receiving the data package in a user's data processor;

storing the data package in a memory device where it is accessible by means of the user's data processor;

decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data;

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage, otherwise disabling it; and

reconcatenating, after the usage of the data object, the data object and the one or more usage control elements of the user set of control data, and reencrypting at least the data object and the one or more usage of the user set of control data.

119. A system for managing a data object so as to comply with control conditions for usage of the data object, comprising:

first means in the data object provider's data processor for creating a general set of control data for the data object based on the predetermined conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the predetermined conditions;

storing means, which are accessible by means of said data processor, for storing the data object and the general set of control data;

concatenating means for concatenating the general set of control data with a copy of the data object;

encrypting means for encrypting the copy of the data object and at least said one or more usage control elements to create a secure data package, which is ready for transfer to a user;

second means in said data processor for creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of said usage control elements;

using the user set of control data instead of the general set of control data in the storing means;

using the user set of control data instead of the general set of control data in the concatenating means;

using the user set of control data instead of the general set of control data in the encrypting means; and

checking means in said data processor for checking that said request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

120. A method for managing an object so as to comply with control conditions for usage of the object, comprising the steps of:

storing the object in a storage device, where it is accessible by means of an object provider's electronic appliance;

providing a variable number of control conditions for usage of the object;
creating, by said electronic appliance, a general set of control data for the object based on said variable number of control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the object which comply with said variable number of control conditions,
storing said general set of control data in a storage device, where it is accessible by said electronic appliance;
containerizing the general set of control data with a copy of the object; and
encrypting at least the copy of the object and said one or more usage control elements to create a secure container which is ready for transfer to a user.

121. A method as set forth in claim 120, wherein the step of encrypting comprises encrypting the object and the general set of control data.

122. A method as set forth in claim 120, wherein the step of creating control data comprises creating an identifier which uniquely identifies the general set of control data.

123. A method as set forth in claim 120, wherein the step of creating a general set of control data comprises creating a security control element which identifies a security process to be applied before usage of the object is allowed.

124. A method as set forth in claim 120, wherein the step of creating a general set of control data comprises creating a format control element which identifies the format of the control data.

125. A method as set forth in claim 120, further comprising the steps of receiving in said electronic appliance a request for authorization for usage by a user; comparing the usage for which authorization is requested with said one or more usage control elements of the general set of control data and granting the authorization if the usage for which authorization is requested complies with the usages defined by said one or more usage control elements.

126. A method as set forth in claim 125, further comprising the step of securing payment for the requested authorization for usage before granting the authorization.

127. A method as set forth in claim 120, comprising the further steps of:

- receiving the container in a user's electronic appliance;
- storing the container in a storage device where it is accessible by means of the user's electronic appliance;
- decrypting said one or more usage control elements;

checking, in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data;

decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the object and enabling the requested usage, otherwise disabling it.

128. A method as set forth in claim 127, comprising the further steps of recontainerizing, after the usage of the object, the object and the one or more usage control elements, reencrypting at least the object and the one or more usage control elements, and storing the thus-recontainerized container in the storage of the user's electronic appliance.

129. A method for controlling the usage by a user of an object so as to comply with control conditions for usage of the object, comprising the steps of:

providing a variable number of control conditions for usage of the object;
storing a container in a storage device, where it is accessible by means of an electronic appliance of the user, said container comprising the object and control data, which comprises at least one usage control element defining a usage of the object which complies with the variable number of control conditions, the object and said at least one usage control element being encrypted;

receiving a request by the user for usage of the object;

decrypting the control data;
checking, in response to the request by the user for usage of the object,
whether the requested usage complies with the usage defined by the at least one usage
control element of the control data; and

decrypting, in response to the requested usage complying with the usage
defined by the at least one usage control element of the control data, the object and
enabling the requested usage, otherwise disabling it.

130. A method as set forth in claim 129, wherein the usage control element is
updated after the at least one usage of the object.

131. A method as set forth in claim 129, wherein said control data comprises an
indication of the number of times the user is authorized to use the object in accordance
with said at least one usage control element;

wherein the requested usage of the object is only enabled when said number of
times is one or more; and

wherein said number of times is decremented by one when the requested usage
is enabled.

132. A method as set forth in claim 129, wherein the control data comprise a security control element, and further comprising the step of carrying out, before each usage of the object, a security procedure defined in the security control element.

133. A method as set forth in claim 129, wherein the step of checking whether the requested usage complies with the usage defined by the at least one usage control element comprises the step of checking that the user's electronic appliance is capable of carrying out a security procedure specified in a security control element of the at least one usage control element, and if not, disabling the usage.

134. A method as set forth in claim 129, comprising the further steps of recontainerizing, after the usage of the object, the object and the one or more usage control elements, reencrypting at least the object and the one or more usage control elements, and storing the thus-recontainerized container in the storage of the user's electronic appliance.

135. A system for managing an object so as to comply with control conditions for usage of the object, comprising means for providing a variable number of control conditions;

first means in the object provider's electronic appliance for creating a general set of control data for the object based on the variable number of control conditions for usage, said general set of control data comprising at least one or more usage control

elements defining usage of the object which comply with the variable number of control data in condition storing means;

storing means, which are accessible by means of the electronic appliance, for in storing the object and the general set of control data;

containing means for containing the general set of control data in a copy of the object; and

encrypting means for encrypting the copy of the object and at least said one or more usage control elements of the object, which is ready for transfer of the user container to the user.--

136. A system as set forth in claim 135, wherein the general set of control data comprises a control data element which defines the right to further distribution of the object by the user.

137. A system for controlling the usage by a user of an object so as to comply with control conditions for usage of the object, comprising:

means for providing variable number of control conditions;

storing means for storing a container which comprises an object and a control data comprising at least one usage control element defying a usage of the object which complies with the variable number of control conditions;

means for decrypting the at least one usage control element and the object;

- recontainerizing, after the usage of the object, the object and the one or more
checking means for checking whether a usage requested by the user complies
usage control elements of the user set of control data, and reencrypting at least the object
with the usage defined by said at least one usage control element;
and the one or more usage of the user set of control data,
enabling means for enabling the usage requested by the user when the usage
complies with the usage defined by said at least one usage control element; and
148. A system for managing an object so as to comply with control conditions for
disabling means for disabling the usage requested by the user when the usage
usage of the object, comprising:
does not comply with the usage defined by said at least one usage control element.
first means in the object provider's electronic appliance for creating a general
set of control data for the object based on the predetermined conditions for usage, said
138. A system as set forth in claim 137, further comprising means for
general set of control data comprising at least one or more usage control elements defining
recontainerizing the object after usage thereof.
usages of the object which comply with the predetermined conditions;
139. A method for controlling the usage by a user of objects so as to comply with
storing means, which are accessible by means of said electronic appliance, for
storing the object and the general set of control data;
predetermined conditions for usage of the objects, comprising the steps of:
containerizing means for containerizing the general set of control data with a
storing at least two containers in a storage device, where they are accessible
copy of the object;
by an electronic appliance of the user, each said container comprising an object and a user
encrypting means for encrypting the copy of the object and at least said one or
set of control data, which comprises at least one usage control element defining a usage of
more usage control elements to create a secure container, which is ready for transfer to a
the object which complies with the predetermined conditions, the object and said at least
user;
one usage control elements being encrypted;
- second means in said electronic appliance for creating, in response to a request
decrypting the usage control elements of the user sets of control data,
for authorization for usage of the object by a user, a user set of control data, which
examining the usage control elements of said at least two containers to find a
comprises at least a subset of the general set of control data, which subset comprises at
match;
least one of said usage control elements;

checking in response to the request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and

140. A method as set forth in claim 139, comprising the further steps of repeating the at least one usage control element of the user set of control data, the object and enabling the requested usage and otherwise disabling it; reencrypting each of the contained objects and its at least one usage control element and transferring the recontainerized objects to the user;

141. A method as set forth in claim 141, further comprising:

receiving the container in a user's electronic appliance;

141. Storing the container in a storage device where it is accessible by means of the user's electronic appliance;

decrypting the object as a usage control element of the user set of control data; and checking in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data; and if the requested usage complies with the usage defined by the at least one usage control element of the user set of control data, the object and enabling the requested usage and otherwise disabling it; and

containerizing the general set of control data with a copy of the object;

comprising the step of transferring the container through the data network to the user's electronic appliance secure container which is ready for transfer to a user;

creating, in response to a request for authorization for usage of the object by a user, a user set of control data, which comprises wherein the object is the composite object including at least one constituent object and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each constituent object and the composite object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each constituent object and the composite object of the general set of control data in the encrypting step; and

145. A method as defined in claim 144, comprising the further step of storing a request for authorization of control data of the object has been granted.

146. A method as defined in claim 141, comprising the further steps of at least two constituent objects the container in a user's electronic appliance; in response to a request for authorization for usage of the container and constituent objects by a user, is created only for that user's electronic appliance maintained only with a copy of that constituent object.

decrypting the at least one usage control element of the user set of control data; 143. A method as set forth in claim 141, wherein the data provider's electronic appliance is connected to a data network and the request for authorization is received from an electronic appliance of the user, which is also connected to the data network, further

comprising the step of transferring the container through the data network to the user's electronic appliance.

144. A method as set forth in claim 141, wherein the object is a composite object including at least two constituent objects and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent objects and the composite object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent objects and the composite object.

145. A method as defined in claim 141, comprising the further step of storing a copy of the user set of control data in the object provider's processor.

146. A method as defined in claim 141, comprising the further steps of:

- receiving the container in a user's electronic appliance;
- storing the container in a storage device where it is accessible by means of the user's electronic appliance;
- decrypting the at least one usage control element of the user set of control data;

checking, in response to a request by the user for usage of the object, whether the requested usage complies with the usage defined by the at least one usage control element to create a secure container which is ready for transfer to a user, element of the user set of control data; and creating, in response to a request for authorization for usage of the object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of said usage control elements, defined by the at least one usage control element of the user set of control data, the object and enabling the requested usage, otherwise disabling it, using the user set of control data instead of the general set of control data in said containerizing step;

147. A method as set forth in claim 141, further comprising: receiving the container in a user's electronic appliance; storing the container in a storage device where it is accessible by means of the user's electronic appliance; checking, before allowing transfer of the container to the user, that said request for authorization for usage of the object has been granted; decrypting the at least one usage control element of the user set of control data;

142. A method as set forth in claim 141, wherein the object is composed of at least two constituent objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent objects by a user, is created only for that constituent object and contains only a copy of that constituent object; decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the object and enabling the requested usage, otherwise disabling it; and

143. A method as set forth in claim 141, wherein the data provider's electronic appliance is connected to a data network and the request for authorization is received from an electronic appliance of the user, which is also connected to the data network, further

using, in response to the finding of a match, the electronic appliance to carry out an action, which is specified in the user sets of control data, and reencrypting at least the object and the one or more usage of the user set of control data.

140. A method as set forth in claim 139, comprising the further steps of updating

the at least one usage control element of each container, containerizing after the usage of the objects, each of the objects and its at least one usage control element, reencrypting each usage of the object, comprising:

of the contained objects and its at least one usage control element and transferring the first means in the object provider's electronic appliance for creating a general set of control data for the object based on the predetermined conditions for usage, said

general set of control data comprising at least one or more usage control elements defining

141. A method for managing an object so as to comply with predetermined usages of the object which comply with the predetermined conditions,

conditions for usage of the object, comprising the steps of:
storing means, which are accessible by means of said electronic appliance, for storing the object in a storage device, where it is accessible by means of an object provider's data processor;

containerizing means for containerizing the general set of control data with a copy of the object;

providing control conditions for usage of the object;

creating, by said electronic appliance, a general set of control data for the object based on said control conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the object which

comply with said control conditions;

second means in said electronic appliance for creating, in response to a request for authorization for usage of the object by a user, a user set of control data, which

accessible by said electronic appliance;
comprises at least a subset of the general set of control data, which subset comprises at least one of said usage control elements;

containerizing the general set of control data with a copy of the object;

checking means for checking whether a usage requested by the user complies with the usage defined by said at least one usage control element;
the storing means,

enabling means for enabling the usage requested by the user when the usage complies with the usage defined by said at least one usage control element; and
the containerizing means,

disabling means for disabling the usage requested by the user when the usage does not comply with the usage defined by said at least one usage control element.
the encrypting means; and

checking means in said electronic appliance for checking that said request for authorization for usage of the object has been granted before allowing transfer of the container to the user.
138. A system as set forth in claim 137, further comprising means for recontainerizing the object after usage thereof.

139. A method for controlling the usage by a user of objects so as to comply with predetermined conditions for usage of the objects, comprising the steps of:

storing at least two containers in a storage device, where they are accessible by an electronic appliance of the user, each said container comprising an object and a user set of control data, which comprises at least one usage control element defining a usage of the object which complies with the predetermined conditions, the object and said at least one usage control elements being encrypted;

decrypting the usage control elements of the user sets of control data;

examining the usage control elements of said at least two containers to find a match;

F

RECEIVED

Form PTO-850 (Rev. 01-10-2001)

INTERFERENCE INITIAL MEMORANDUM

Count # 1

To the Board of Patent Appeals and Interferences:

An interference is proposed involving the following 2 parties—

PARTY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
✓ Ginter et al.	09/411205	10/4/99	—	—

If the involved case is a patent, have its maintenance fees been paid? Yes ☐ No ☐ Not due yet ☐

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
USA	09/208017	12/9/98	6253193	6/26/01
USA	08/964333	11/4/97	5982891 5842891	11/9/99 4/6/97
USA	08/388107	2/13/95	—	—

The claim(s) of this party corresponding to this count: 91-93, 95-102, 105-109, 112-122, 124-131, 134-138, 141-148

PATENTED OR PATENTABLE PENDING CLAIMS	all	UNPATENTABLE PENDING CLAIMS	—
---------------------------------------	-----	-----------------------------	---

The claim(s) of this party NOT corresponding to this count: 94, 103, 104, 110, 111, 123, 132, 133, 139, 140

PATENTED OR PATENTABLE PENDING CLAIMS	all	UNPATENTABLE PENDING CLAIMS	—
---------------------------------------	-----	-----------------------------	---

PARTY (Benson I)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
✓ Benson et al.	08/594811	1/31/96	5845281	12/1/98

If the involved case is a patent, have its maintenance fees been paid? Yes ☒ No ☐ Not due yet ☐ 4/8/02 3 1/2 yr. fee paid

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY

The claim(s) of this party corresponding to this count: 1-3, 5-12, 15-19, 22-29

PATENTED OR PATENTABLE PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>		
The claim(s) of this party NOT corresponding to this count: 4, 13, 14, 20, 21			
PATENTED OR PATENTABLE PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>		
(Check off each step, if applicable) INSTRUCTIONS			
<ul style="list-style-type: none"> 1. Obtain all files listed above. 2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970). 3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b). 4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)). 5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center. 			
DATE	PRIMARY EXAMINER (signature)	ART UNIT	TELEPHONE NO.
DATE	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature)		TELEPHONE NO.
			Page <u>1</u> of <u>6</u>

RECEIVED

Form PTO-850-(Rev. 01-10-2001)		INTERFERENCE INITIAL MEMORANDUM			Count # <u>1</u>
To the Board of Patent Appeals and Interferences:					
An interference is proposed involving the following <u>2</u> parties—					
PARTY (Benson II)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
✓ Benson et al.	09/164 606	10/1/98	—	—	
If the involved case is a patent, have its maintenance fees been paid? Yes <input type="checkbox"/> No <input type="checkbox"/> Not due yet <input type="checkbox"/>					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
USA	08/594811	1/31/96	5845281	12/1/98	
The claim(s) of this party corresponding to this count: <u>30-32, 34-41, 44-46, 48, 51, 56, 58-66, 68, 69</u>					
PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS			UNPATENTABLE PENDING CLAIMS		
<u>all</u>			—		
The claim(s) of this party NOT corresponding to this count: <u>33, 42, 43, 47, 49, 50, 52-55, 57, 67</u>					
PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS			UNPATENTABLE PENDING CLAIMS		
<u>all</u>			—		
PARTY (Benson III)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
✓ Benson et al.	09/321 386	5/27/99	—	—	
If the involved case is a patent, have its maintenance fees been paid? Yes <input type="checkbox"/> No <input type="checkbox"/> Not due yet <input type="checkbox"/>					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
USA	09/164606	10/1/98	—	—	
USA	08/594811	1/31/96	5845281	12/1/98	
The claim(s) of this party corresponding to this count: <u>1-3, 5-12, 15-17, 19, 22, 27, 29-37, 39-53</u>					

PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>
The claim(s) of this party NOT corresponding to this count: <u>4, 13, 14, 18, 20, 21, 23-26, 28, 38</u>	
PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>
(Check off each step, if applicable) INSTRUCTIONS	
<ul style="list-style-type: none"> 1. Obtain all files listed above. 2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970). 3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b). 4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)). 5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center. 	
DATE <div style="font-size: 1.2em;">8/22/03</div>	PRIMARY EXAMINER (signature) <div style="font-family: cursive; font-size: 1.2em;">Maria N. Von Buh</div>
DATE <div style="font-size: 1.2em;">8/22/03</div>	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature) <div style="font-family: cursive; font-size: 1.2em;">Rick L. Lauer</div>
ART UNIT <div style="font-size: 1.2em;">2125</div>	TELEPHONE NO. <div style="font-size: 1.2em;">305-3837</div>
TELEPHONE NO. <div style="font-size: 1.2em;">306-4160</div>	
Page <u>2</u> of <u>6</u>	

RECEIVED

Form PTO-850 (Rev. 01-10-2001)		INTERFERENCE INITIAL MEMORANDUM			Count # <u>2</u>
To the Board of Patent Appeals and Interferences:					
An interference is proposed involving the following <u>2</u> parties—					
PARTY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
Ginter et al.	09/411205	10/4/99	—	—	
If the involved case is a patent, have its maintenance fees been paid? Yes <input type="checkbox"/> No <input type="checkbox"/> Not due yet <input type="checkbox"/>					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
USA	09/208017	12/9/98	6253193	6/26/01	
USA	08/964333	11/4/97	5892891	4/6/99	
USA	08/388107	2/13/95	—	—	
The claim(s) of this party corresponding to this count: <u>94, 103, 104, 123, 132, 133</u>					
PATENTED OR PATENTABLE PENDING CLAIMS			UNPATENTABLE PENDING CLAIMS		
<u>all</u>			—		
The claim(s) of this party NOT corresponding to this count: <u>91-93, 95-102, 105-122, 124-131, 134-148</u>					
PATENTED OR PATENTABLE PENDING CLAIMS			UNPATENTABLE PENDING CLAIMS		
<u>all</u>			—		
PARTY (Benson I)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
Benson et al.	08/594811	1/31/96	5845281	12/1/98	
If the involved case is a patent, have its maintenance fees been paid? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Not due yet <input type="checkbox"/> <u>4/8/02 3 1/2 yr. fee paid</u>					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
The claim(s) of this party corresponding to this count: <u>4, 13, 14</u>					

PATENTED OR PATENTABLE PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>		
The claim(s) of this party NOT corresponding to this count: 1-3, 5-12, 15-29			
PATENTED OR PATENTABLE PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>		
(Check off each step, if applicable) INSTRUCTIONS			
<ul style="list-style-type: none"> 1. Obtain all files listed above. 2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970). 3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b). 4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)). 5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center. 			
DATE	PRIMARY EXAMINER (signature)	ART UNIT	TELEPHONE NO.
DATE	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature)	TELEPHONE NO.	
			Page <u>3</u> of <u>6</u>

RECEIVED

Form PTO-850-(Rev. 01-10-2001)		INTERFERENCE INITIAL MEMORANDUM			NOV 25 1998 Mail # 42
To the Board of Patent Appeals and Interferences:					APPEAL REFERENCES
An interference is proposed involving the following <u>2</u> parties—					
PARTY (Benson II) <i>Benson et al.</i>	APPLICATION NO. <i>09/164 606</i>	FILING DATE <i>10/1/98</i>	PATENT NO., IF ANY —	ISSUE DATE, IF ANY —	
If the involved case is a patent, have its maintenance fees been paid? Yes ___ No ___ Not due yet ___					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
<i>USA</i>	<i>08/594 811</i>	<i>1/31/96</i>	<i>5845 281</i>	<i>12/1/98</i>	
The claim(s) of this party corresponding to this count: <i>33, 42, 43, 47, 49, 50, 57, 67</i>					
PATENTED OR PATENTABLE PENDING CLAIMS <i>all</i>			UNPATENTABLE PENDING CLAIMS —		
The claim(s) of this party NOT corresponding to this count: <i>30-32, 34-41, 44-46, 48, 51-56, 58-66, 68, 69</i>					
PATENTED OR PATENTABLE PENDING CLAIMS <i>all</i>			UNPATENTABLE PENDING CLAIMS —		
PARTY (Benson III) <i>Benson et al.</i>	APPLICATION NO. <i>09/321 386</i>	FILING DATE <i>5/27/99</i>	PATENT NO., IF ANY —	ISSUE DATE, IF ANY —	
If the involved case is a patent, have its maintenance fees been paid? Yes ___ No ___ Not due yet ___					
Proposed priority benefit (list all intervening applications necessary for continuity):					
COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY	
<i>USA</i>	<i>09/164 606</i>	<i>10/1/98</i>	—	—	
<i>USA</i>	<i>08/594 811</i>	<i>1/31/96</i>	<i>5845 281</i>	<i>12/1/98</i>	
The claim(s) of this party corresponding to this count: <i>4, 13, 14, 18, 20, 21, 28, 38</i>					

PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>
The claim(s) of this party NOT corresponding to this count: 1-3, 5-12, 15-17, 19, 22-27, 29-37, 39-53	
PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center; font-size: 1.2em;">all</div>	UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>
(Check off each step, if applicable) INSTRUCTIONS	
<ul style="list-style-type: none"> 1. Obtain all files listed above. 2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970). 3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b). 4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)). 5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center. 	
DATE <div style="font-size: 1.2em;">8/22/03</div>	PRIMARY EXAMINER (signature) <div style="font-family: cursive; font-size: 1.2em;">Maria M. Von Bueh</div>
DATE <div style="font-size: 1.2em;">8/22/03</div>	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature) <div style="font-family: cursive; font-size: 1.2em;">Paul E. Luffer</div>
ART UNIT <div style="font-size: 1.2em;">2125</div>	TELEPHONE NO. <div style="font-size: 1.2em;">305-3837</div>
TELEPHONE NO. <div style="font-size: 1.2em;">306-4460</div>	
Page <u>4</u> of <u>6</u>	

RECEIVED

Form PTO-850 (Rev.
01-10-2001)

INTERFERENCE INITIAL MEMORANDUM

Count # 13

To the Board of Patent Appeals and Interferences:

An interference is proposed involving the following 2 parties—

PARTY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
Ginter et al.	09/411205	10/4/99	—	—

If the involved case is a patent, have its maintenance fees been paid? Yes ___ No ___ Not due yet ___

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
USA	09/208017	12/9/98	6253193	6/26/01
USA	08/964333	11/4/97	5892891	4/6/99
USA	08/388107	2/13/95	—	—

The claim(s) of this party corresponding to this count: 110, 111, 139, 140

PATENTED OR PATENTABLE PENDING CLAIMS

all

UNPATENTABLE PENDING CLAIMS

—

The claim(s) of this party NOT corresponding to this count: 91-109, 112-138, 141-148

PATENTED OR PATENTABLE PENDING CLAIMS

all

UNPATENTABLE PENDING CLAIMS

—

PARTY (Benson I)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
Benson et al.	08/594811	1/31/96	5845281	12/1/98

If the involved case is a patent, have its maintenance fees been paid? Yes X No ___ Not due yet 4/8/02 3 1/2 yr. fee paid

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY

The claim(s) of this party corresponding to this count:

20, 21

PATENTED OR PATENTABLE PENDING CLAIMS all		UNPATENTABLE PENDING CLAIMS —	
The claim(s) of this party NOT corresponding to this count: 1-19, 22-29			
PATENTED OR PATENTABLE PENDING CLAIMS all		UNPATENTABLE PENDING CLAIMS —	
(Check off each step, if applicable) INSTRUCTIONS			
<ul style="list-style-type: none">1. Obtain all files listed above.2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970).3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b).4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)).5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center.			
DATE	PRIMARY EXAMINER (signature)	ART UNIT	TELEPHONE NO.
DATE	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature)		TELEPHONE NO.
			Page 5 of 6

Form PTO-850 (Rev.
01-10-2001)

INTERFERENCE INITIAL MEMORANDUM

195 AM Count 3

To the Board of Patent Appeals and Interferences:

An interference is proposed involving the following 2 parties—

PARTY (Benson II)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
Benson et al.	09/164606	10/1/98	—	—

If the involved case is a patent, have its maintenance fees been paid? Yes ☐ No ☐ Not due yet ☐

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
USA	08/594811	1/31/96	5845 281	12/1/98

The claim(s) of this party corresponding to this count: 52, 53, 55

PATENTED OR PATENTABLE PENDING CLAIMS

all

UNPATENTABLE PENDING CLAIMS

—

The claim(s) of this party NOT corresponding to this count:

30-51, 54, 56-69

PATENTED OR PATENTABLE PENDING CLAIMS

all

UNPATENTABLE PENDING CLAIMS

—

PARTY (Benson III)	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
Benson et al.	09/321 386	5/27/99	—	—

If the involved case is a patent, have its maintenance fees been paid? Yes ☐ No ☐ Not due yet ☐

Proposed priority benefit (list all intervening applications necessary for continuity):

COUNTRY	APPLICATION NO.	FILING DATE	PATENT NO., IF ANY	ISSUE DATE, IF ANY
USA	09/164606	10/1/98	—	—
USA	08/594811	1/31/96	5845 281	12/1/98

The claim(s) of this party corresponding to this count:

23, 24

PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center;">all</div>		UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>	
The claim(s) of this party NOT corresponding to this count: <div style="text-align: center;">1-22, 25-53</div>			
PATENTED OR <u>PATENTABLE</u> PENDING CLAIMS <div style="text-align: center;">all</div>		UNPATENTABLE PENDING CLAIMS <div style="text-align: center;">—</div>	
(Check off each step, if applicable) INSTRUCTIONS			
<ul style="list-style-type: none">• 1. Obtain all files listed above.• 2. Confirm that the proposed involved claims are still active and all corrections and entered amendments have been considered. The patents must not be expired for, among other things, failure to pay a maintenance fee (Check PALM screen 2970).• 3. If one of the involved files is a published application or a patent, check for compliance with 35 U.S.C. 135(b).• 4. Obtain a certified copy of any foreign benefit documents where necessary (37 CFR 1.55(a)).• 5. Discuss the proposed interference with an Interference Practice Specialist in your Technology Center.			
DATE <div style="text-align: center;">8/22/03</div>	PRIMARY EXAMINER (signature) <div style="text-align: center;"><i>Maria N. VonBehr</i></div>	ART UNIT <div style="text-align: center;">2125</div>	TELEPHONE NO. <div style="text-align: center;">305-3837</div>
DATE <div style="text-align: center;">8/22/03</div>	INTERFERENCE PRACTICE SPECIALIST or TECHNOLOGY CENTER DIRECTOR (signature) <div style="text-align: center;"><i>Paul S. Laufer</i></div>	TELEPHONE NO. <div style="text-align: center;">306-4160</div>	
Page <u>6</u> of <u>6</u>			

Interference #xxxxxx

1. **Count 1:** Claim 1 of SN 09/321,386 (Benson et al. III).
2. **Count 2:** Claim 4 of SN 09/321,386 (Benson et al. III).
3. **Count 3:** Claim 23 of SN 09/321,386 (Benson et al. III).

Differences between the counts:

Count 2 depends from Count 1, but the specific security control elements, and processing in response thereto, of Count 2 would not have been obvious over the presence of generic control elements in the method of Count 1.

Count 3 is separate from Count 1, because the comparing of multiple data packages for matching elements in order to control processor execution of Count 3 would not have been obvious over using control elements to control access to data objects as in the method of Count 1.

Means plus function analysis:

No means plus function language has been used.

Correlation of claims in SN 09/321,386 (Benson et al. III), SN 09/164,606 (Benson et al. II), PN 5845281 (Benson et al. I) and SN 09/411,205 (Ginter et al., Senior party) to the counts:

COUNT 1:

- claim 1 of SN 09/321,386 (Benson et al. III), with the following corresponding claims:
SN 09/321,386 (Benson et al. III): claims 1-3, 5-12, 15-17, 19, 22, 27, 29-37 and 39-53
SN 09/164,606 (Benson et al. II): claims 30-32, 34-41, 44-46, 48, 51, 56, 58-66, 68 and 69
PN 5845281 (Benson et al. I): claims 1-3, 5-12, 15-19 and 22-29
SN 09/411,205 (Ginter et al.): claims 91-93, 95-102, 105-109, 112-122, 124-131, 134-138 and 141-148

Correspondence of claims of SN 09/321,386 (Benson et al. III) to Count 1 above.

Independent claim 1 is Count 1.

Independent claim 10 provides for the "mirror" of the method of Count 1 (i.e.; Count 1 provides for packaging of a data object with its usage control elements for transmission to a user, while this claim provides for the user receiving such objects and using them according to the usage control elements), which would have been an obvious consequence of the method of Count 1.

Independent claim 16 is the apparatus version of Count 1.

Independent claim 19 is the apparatus version of claim 10, similar to the method of Count 1 as noted above.

Independent claims 27 and 35 provide for repeated (re)-packaging of the data objects (i.e.; the sharing of data objects) of the method of Count 1, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in such a shared data environment, for example.

Independent claims 36, 41, 43 and 48, and claims 37, 42, 44 and 50, are similar to the method of Count 1 except that various steps have been omitted, such being obvious since omission of an element and its function in a combination where remaining elements perform the same functions as before involves only routine skill in the art.

Claim 2 adds the limitation that the general set of control data is also encrypted. Such a modification would have been obvious, to one having ordinary skill in the art, at the time the instant invention was made, because encrypting control data was well-known to enhance overall security of data distribution (for example: taught at least by Hellman, U.S. PN 4658093, see at least claim 5; and Wiedemer, U.S. PN 4796181, see at least col. 13).

Claims 3, 5, 17, 39 and 52 add limitations concerning various types of control data included in the method of Count 1, which would have been obvious choices, to one having ordinary skill in the art, at the time the instant invention was made, as a consequence of implementation in particular well-known data distribution environments.

Claims 6, 8, 33, 40 and 49 additionally provide for the "mirror" of the method of Count 1 (i.e.; Count 1 provides for the packaging of a data object with its usage control elements for transmission to a user, while these listed claims provide for the user receiving such objects and using them according to the usage control elements), which would have been an obvious consequence of the method of Count 1.

Claim 7 adds the limitation of requiring payment to the method of Count 1, which would have been an obvious variation, in view of the well-known application of data object management to a licensing/Internet environment, for example.

Claims 9, 15, 22, 32 and 34 additionally provide for repeated (re)-packaging of the data objects (i.e.; the sharing of data objects) of the method of Count 1, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in such a shared data environment, for example.

Claims 11 and 12 provide additional limitations concerning updating of usage control elements (i.e.; decrementing number of uses), which would have been implementation specific, and obvious to one having ordinary skill in the art, at the time the instant invention was made, since number of uses was a well-known criteria for shared data control.

Claims 29 and 31 add limitations concerning plural objects being grouped within a package of the method of Count 1, which would have been an obvious variation, at the time the instant invention was made, in view of bandwidth considerations for network data transmission (i.e.; it was well-known in the art to packetize data for transmission in a network, in order to reduce bandwidth requirements).

Claim 30 adds the limitation that transmission of a data package of the method of Count 1 is across a network, such network transmission of data having been well-known at the time the instant invention was made.

Claims 45-47, 51 and 53 add limitations concerning various types of data enclosed in (i.e.; the contents of) the packages of the method of Count 1, all of which would have been obvious choices, to one having ordinary skill in the art, as a consequence of implementation in particular well-known data distribution environments.

Correspondence of claims of SN 09/164,606 (Benson et al. II) to Count 1 above.

Independent claims 30, 39, 56, 64 and 65, and claims 31 and 66, include all the limitations of the method of Count 1, while adding the limitation that the general set of control data is also encrypted. Such a modification would have been obvious, to one having ordinary skill in the art, at the time the instant invention was made, because encrypting control data was well-known to enhance overall security of data distribution (for example: taught at least by Hellman, U.S. PN 4658093, see at least claim 5; and Wiedemer, U.S. PN 4796181, see at least col. 13).

Independent claim 45 is the apparatus version of claim 30, similar to the method of Count 1 as noted above.

Independent claim 48 is the apparatus version of claim 39, similar to the method of Count 1 as noted above.

Claims 32, 34, 46 and 68 add limitations concerning various types of control data included in the method of Count 1, all of which would have been obvious choices, to one having ordinary skill in the art, at the time the instant invention was made, as a consequence of implementation in particular well-known data distribution environments.

Claims 35, 37, 62 and 69, and additionally claims 39 and 48, provide for the "mirror" of the method of Count 1 (i.e.; Count 1 provides for the packaging of a data object with its usage control elements for transmission to a user, while these listed claims provide for the user receiving such objects and using them according to the usage control elements), which would have been an obvious consequence of the method of Count 1.

Claim 36 adds the limitation of requiring payment to the method of Count 1, which would have been an obvious variation, in view of the well-known application of data object management to a licensing/Internet environment, for example.

Claims 38, 44, 51, 61 and 63, and additionally claims 56 and 64, provide for repeated (re)-packaging of the data objects (i.e.; the sharing of data objects) of the method of Count 1, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in such a shared data environment, for example.

Claims 40 and 41 provide additional limitations concerning updating of usage control elements (i.e.; decrementing number of uses), which would have been implementation specific, and obvious to one having ordinary skill in the art, at the time the instant invention was made, since number of uses was a well-known criteria for shared data control.

Claims 58 and 60 add limitations concerning plural objects being grouped within a package of the method of Count 1, which would have been an obvious variation, at the time the instant invention was made, in view of bandwidth considerations for network data transmission (i.e.; it was well-known in the art to packetize data for transmission in a network, in order to reduce bandwidth requirements).

Claim 59 adds the limitation that transmission of a data package of the method of Count 1 is across a network, such network transmission of data having been well-known at the time the instant invention was made.

Correspondence of claims of PN 5845281 (Benson et al. I) to Count 1 above.

Independent claims 1, 10, 22 and 29, and claim 2, include all the limitations of the method of Count 1, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage.

Independent claim 16 is the apparatus version of the method of claim 1, similar to Count 1 as noted above.

Independent claim 18 is the apparatus version of the method of claim 10, similar to Count 1 as noted above.

Claims 3, 5 and 17 add limitations concerning various types of control data included in the method of Count 1, all of which would have been obvious choices, to one having ordinary skill in the art, at the time the instant invention was made, as a consequence of implementation in particular well-known data distribution environments.

Claims 6, 8 and 27, and additionally claims 10 and 18, provide for the "mirror" of the method of Count 1 (i.e.; Count 1 provides for the packaging of a data object with its usage control elements for transmission to a user, while these listed claims provide for the user receiving such objects and using them according to the usage control elements), which would have been an obvious consequence of the method of Count 1.

Claim 7 adds the limitation of requiring payment to the method of Count 1, which would have been an obvious variation, in view of the well-known application of data object management to a licensing/Internet environment, for example.

Claims 9, 15, 19, 26 and 28, and additionally claims 22 and 29, provide for repeated (re)-packaging of the data objects (i.e.; the sharing of data objects) of the method of Count 1, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in such a shared data environment, for example.

Claims 11 and 12 provide additional limitations concerning updating of usage control elements (i.e.; decrementing number of uses), which would have been implementation specific, and obvious to one having ordinary skill in the art, at the time the instant invention was made, since number of uses was a well-known criteria for shared data control.

Claims 23 and 25 add limitations concerning plural objects being grouped within a package of the method of Count 1, which would have been an obvious variation, at the time the instant invention was made, in view of bandwidth considerations for network data transmission (i.e.; it was well-known in the art to packetize data for transmission in a network, in order to reduce bandwidth requirements).

Claim 24 adds the limitation that transmission of a data package of the method of Count 1 is across a network, such network transmission of data having been well-known at the time the instant invention was made.

Correspondence of claims of SN 09/411,205 (Ginter et al.) to Count 1 above.

Claims 91-93, 95-102, 105-109 and 112-119 are identical to claims 1-3, 5-12, 15-19 and 22-29 of PN 5845281 (Benson et al. I) above. Accordingly, the following applies:

Independent claims 91, 100, 112 and 119, and claim 92, include all the limitations of the method of Count 1, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage.

Independent claim 106 is the apparatus version of the method of claim 91, similar to Count 1 as noted above.

Independent claim 108 is the apparatus version of the method of claim 100, similar to Count 1 as noted above.

Claim 120 is substantially similar to the method of Count 1, except that equivalent language from the specification of Ginter et al. has been used.

Claim 135 is the apparatus version of claim 120, similar to the method of Count 1 as noted above.

Claims 93, 95 and 107 add limitations concerning various types of control data included in the method of Count 1, all of which would have been obvious choices, to one having ordinary skill in the art, at the time the instant invention was made, as a consequence of implementation in particular well-known data distribution environments. Corresponding claims 121, 122, 124 and 136 use the equivalent language noted above.

Claims 96, 98 and 117, and additionally claims 100 and 108, provide for the "mirror" of the method of Count 1 (i.e.; Count 1 provides for the packaging of a data object with its usage control elements for transmission to a user, while these listed claims provide for the user receiving such objects and using them according to the usage control elements), which would have been an obvious consequence of the method of Count 1. Corresponding claims 125, 127, 129, 137 and 146 use the equivalent language noted above.

Claim 97 adds the limitation of requiring payment to the method of Count 1, which would have been an obvious variation, in view of the well-known application of data object management to a licensing/Internet environment, for example. Corresponding claim 126 uses the equivalent language noted above.

Claims 99, 105, 109, 116 and 118, and additionally claims 112 and 119, provide for repeated (re)-packaging of the data objects (i.e.; the sharing of data objects) of the method of Count 1, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in such a shared data environment, for example. Corresponding claims 128, 134, 138, 141, 145, 147 and 148 use the equivalent language noted above.

Claims 101 and 102 provide additional limitations concerning updating of usage control elements (i.e.; decrementing number of uses), which would have been implementation specific, and obvious to one having ordinary skill in the art, at the time the instant invention was made, since number of uses was a well-known criteria for shared data control. Corresponding claims 130 and 131 use the equivalent language noted above.

Claims 113 and 115 add limitations concerning plural objects being grouped within a package of the method of Count 1, which would have been an obvious variation, at the time the instant invention was made, in view of bandwidth considerations for network data transmission (i.e.; it was well-known in the art to packetize data for transmission in a network, in order to reduce bandwidth requirements). Corresponding claims 142 and 144 use the equivalent language noted above.

Claim 114 adds the limitation that transmission of a data package of the method of Count 1 is across a network, such network transmission of data having been well-known at the time the instant invention was made. Corresponding claim 143 uses the equivalent language noted above.

COUNT 2:

- claim 4 of SN 09/321,386 (Benson et al. III), with the following corresponding claims:
SN 09/321,386 (Benson et al. III): claims 4, 13, 14, 18, 20, 21, 28 and 38
SN 09/164,606 (Benson et al. II): claims 33, 42, 43, 47, 49, 50, 57 and 67
PN 5845281 (Benson et al. I): claims 4, 13 and 14
SN 09/411,205 (Ginter et al.): claims 94, 103, 104, 123, 132 and 133

** Since the claims of this count are dependent upon the claims of Count 1, the following analysis tracks Count 1 precisely, with regard to the relationship between the claims in Benson et al. I, II and III. The rationales have been repeated here, with appropriate claim numbering.

Correspondence of claims of SN 09/321,386 (Benson et al. III) to Count 2 above.

Dependent claim 4 is Count 2.

Dependent claim 13 is substantially similar to Count 2, except that it depends from parent claim 10, which differs from parent Count 1 as specified above. Namely, the "mirror" of the method of parent Count 1 was provided for, which would have been an obvious consequence of the method of parent Count 1.

Dependent claims 14 and 28 add the limitation that processor execution is dependent upon the control data, which is an inherent purpose of using control data.

Dependent claim 18 is the apparatus version of claim 4, similar to the method of Count 2 as noted above.

Dependent claim 20 is the apparatus version of claim 13, similar to the method of Count 2 as noted above.

Dependent claim 21 adds the limitation that the encryption uses a specific type of algorithm, which was a well-known type of algorithm at the time the instant invention was made. As admitted by Applicant, at page 10 of the instant specification, it was well-known in the art to use "any appropriate, commercially available [encryption] module."

Dependent claim 38 is substantially similar to the method of Count 2, except that it depends from parent claim 36, which differs from parent Count 1 as specified above. Namely, various steps of storing and/or concatenating are omitted, such being obvious since omission of an element and its function in a combination where the remaining elements perform the same functions as before involves only routine skill in the art.

Correspondence of claims of SN 09/164,606 (Benson et al. II) to Count 2 above.

Dependent claim 33 includes all the limitations of the method of Count 1, while adding the limitation that the general set of control data is also encrypted. Such a modification would have been obvious, to one having ordinary skill in the art, at the time the instant invention was made, because encrypting control data was well-known to enhance overall security of data distribution (for example: taught at least by Hellman, U.S. PN 4658093, see at least claim 5; and Wiedemer, U.S. PN 4796181, see at least col. 13).

Dependent claim 42 is substantially similar to Count 2, except that it depends from parent claim 39, which differs from parent Count 1 as specified above. Namely, the "mirror" of the method of parent Count 1 was provided for, which would have been an obvious consequence of the method of parent Count 1.

Dependent claims 43 and 57 add the limitation that processor execution is dependent upon the control data, which is an inherent purpose of using control data.

Dependent claim 47 is the apparatus version of the method of claim 33, similar to Count 2 as noted above.

Dependent claim 49 is the apparatus version of the method of claim 42, similar to Count 2 as noted above.

Dependent claim 50 adds the limitation that the encryption uses a specific type of algorithm, which was a well-known type of algorithm at the time the instant invention was made. As admitted by Applicant, at page 10 of the instant specification, it was well-known in the art to use "any appropriate, commercially available [encryption] module."

Dependent claim 67 is substantially similar to the method of Count 2, except that it depends from parent claim 65 which differs from parent Count 1 as specified above. Namely, various steps of storing and/or concatenating are omitted, such being obvious since omission of an element and its function in a combination where the remaining elements perform the same functions as before involves only routine skill in the art.

Correspondence of claims of PN 5845281 (Benson et al. I) to Count 2 above.

Dependent claim 4 includes all the limitations of the method of Count 2, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage.

Dependent claim 13 is substantially similar to Count 2, except that it depends from parent claim 10, which differs from parent Count 1 as specified above. Namely, the "mirror" of the method of parent Count 1 was provided for, which would have been an obvious consequence of the method of parent Count 1.

Dependent claim 14 adds the limitation that processor execution is dependent upon the control data, which is an inherent purpose of using control data.

Correspondence of claims of SN 09/411,205 (Ginter et al.) to Count 2 above.

Dependent claims 94, 103 and 104 are identical to claims 4, 13 and 14 of PN 5845281 (Benson et al. I) above. Accordingly, the following applies:

Dependent claim 94 includes all the limitations of the method of Count 2, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage. is identical to Count 2.

Dependent claim 123 is substantially similar to the method of Count 2, except that equivalent language from the specification of Ginter et al. has been used.

Dependent claim 103 is substantially similar to the method of Count 2, except that it depends from parent claim 100, which differs from parent Count 2 as specified above. Namely, the "mirror" of the method of parent Count 2 was provided for, which would have been an obvious consequence of the method of parent Count 2. Corresponding claim 132 uses the equivalent language noted above.

Dependent claim 104 adds the limitation that processor execution is dependent upon the control data, which is an inherent purpose of using control data. Corresponding claim 133 uses the equivalent language noted above.

COUNT 3: **23**

- claim ~~20~~ of SN 09/321,386 (Benson et al. III), with the following corresponding claims:

SN 09/321,386 (Benson et al. III): claims 23 and 24

SN 09/164,606 (Benson et al. II): claims 52, 53 and 55

PN 5845281 (Benson et al. I): claims 20 and 21

SN 09/411,205 (Ginter et al.): claims 110, 111, 139 and 140

** Again, although these claims are independent of the claims in Count 1, the following analysis still tracks Counts 1 and 2 precisely, with regard to the relationship between the claims in Benson et al. I, II and III. The rationales have been repeated here, with appropriate claim numbering.

AJS
Lee
9/2/03

Correspondence of claims of SN 09/321,386 (Benson et al. III) to Count 3 above.

Independent claim 23 is Count 3.

Claim 24 adds a limitation concerning various types of data enclosed in the packages of the method of Count 3, all of which would have been obvious choices, to one having ordinary skill in the art, as a consequence of implementation in a particular data sharing environment.

Correspondence of claims of SN 09/164,606 (Benson et al. II) to Count 3 above.

Independent claim 52 includes all the limitations of the method of Count 3, while adding the limitation that the general set of control data is also encrypted. Such a modification would have been obvious, to one having ordinary skill in the art, at the time the instant invention was made, because encrypting control data was well-known to enhance overall security of data distribution (for example: taught at least by Hellman, U.S. PN 4658093, see at least claim 5; and Wiedemer, U.S. PN 4796181, see at least col. 13).

Claim 53 adds a limitation concerning various types of data enclosed in the packages of the method of Count 3, all of which would have been obvious choices of design, to one having ordinary skill in the art, as a consequence of implementation in a particular environment.

Claim 55 additionally provides for repeated (re)-packaging of the data objects of the method of Count 3, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in a shared data environment, for example.

Correspondence of claims of PN 5845281 (Benson et al. I) to Count 3 above.

Independent claim 20 includes all the limitations of the method of Count 3, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage.

Claim 21 additionally provides for repeated (re)-packaging of the data objects of the method of Count 3, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in a shared data environment, for example.

Correspondence of claims of SN 09/411,205 (Ginter et al.) to Count 3 above.

Claims 110 and 111 are identical to claims 20 and 21 of PN 5845281 (Benson et al. I) above. Accordingly, the following applies:

Independent claim 110 includes all the limitations of the method of Count 2, while adding two limitations. The first limitation provides that the general set of control data is also encrypted. As presented above, with regard to Benson et al. II, such a modification would have been obvious. **Additionally**, the second added limitation provides that data objects and usage control data are stored in memory. Such would have been inherent to any data distribution environment, since the purpose of distribution is for accessibility and use of the data, which would not be possible without some form of storage.

Independent claim 139 is substantially similar to the method of Count 3, except that equivalent language from the specification of Ginter et al. has been used.

Claim 111 provides for repeated (re)-packaging of the data objects of the method of Count 3, wherein such would have been an obvious variation for the well-known purpose of providing versatility and accessibility of the data objects in a shared data environment, for example. Corresponding claim 140 uses the equivalent language noted above.

****NOTE:** claim 54 of SN 09/164,606 (Benson et al. II) and claims 25 and 26 of SN 09/321,386 (Benson et al. III) do not have corresponding interfering claims in SN 09/411,205 (Ginter et al.).

Correlation of claims in application copied from PN 5845281 to claims in patent:

Appl. S.N. 09/411,205 (Ginter et al.)

PN 5845281 (Benson et al. I)

91	1
92	2
93	3
94	4
95	5
96	6
97	7
98	8
99	9
100	10
101	11
102	12
103	13
104	14
105	15
106	16
107	17
108	18
109	19
110	20
111	21
112	22
113	23
114	24
115	25
116	26
117	27
118	28
119	29

G

Paper 1

Filed by: Jameson Lee
Administrative Patent Judge
Mail Stop Interference
P.O. Box 1450
Alexandria VA 22313-1450
Tel: 703-308-9797
Fax: 703-305-0942

Filed
18 December 2003

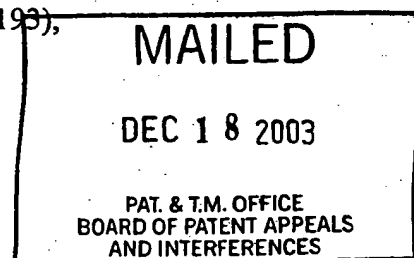
UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

KARL L. GINTER, VICTOR H. SHEAR,
FRANCES J. SPAHN and DAVID M. VAN WIE,
Junior Party,
(Patents 5,920,861; 5,982,891; 6,138,119 and 6,253,193),

v.

GREG BENSON, GREGORY H. URICH
and CHRISTOPHER L. KNAUFT,
Senior Party,
(Applications 09/164,606 and 09/321,386).



Patent Interference No. 105,193

NOTICE DECLARING INTERFERENCE
(37 CFR § 1.611)

Part A. Declaration of interference

An interference is declared (35 U.S.C. § 135(a)) between the above-identified parties.

Details of the application(s), patent (if any), reissue application (if any), count(s) and claims designated as corresponding or as not corresponding to the count(s) appear in Parts E and F of this NOTICE DECLARING INTERFERENCE.

Part B. Judge designated to handle the interference

Administrative Patent Judge Jameson Lee has been designated to handle the interference.

37 CFR § 1.610(a).

Part C. Standing order

A Trial Section STANDING ORDER accompanies this NOTICE DECLARING INTERFERENCE. The STANDING ORDER applies to this interference.

Part D. Conference call to set dates

A telephone conference call to discuss whether the priority phase of this interference can or should be conducted first is scheduled for 1:30 p.m. on 7 January 2004 (the call will be initiated from the PTO).

If the priority phase of this interference is not conducted first, the Administrative Patent Judge intends to set the times for filing preliminary motions on January 7, 2004 and set Time Period 8 as October 7, 2004.

A copy of a "sample" order setting times for taking action during the preliminary motion phase of the interference accompanies this NOTICE DECLARING INTERFERENCE. Counsel are encouraged to discuss the order prior to the conference call with the view to coming to some agreement as to dates for taking action. A typical preliminary motion period lasts approximately nine (9) months. Counsel should be prepared to justify any request for a shorter or longer period.

Part E. The parties involved in this interference are:

Junior Party

Named Inventor: KARL L. GINTER, Beltsville, MD
VICTOR H. SHEAR, Bethesda, MD
FRANCIS J. SPAHN, El Cerrito, CA
DAVID M. VAN WIE, Sunnyvale, CA

Patent: 5,920,861, granted 6 July 1999, based on
application 08/805,804, filed 25 February 1997

Title: Techniques for defining using and manipulating
rights management data structures

Assignee: InterTrust Technologies Corp.

Accorded Benefit: None

Attorneys: See last page

Address: See last page

Patent: 5,982,891, granted 9 November 1999, based on
application 08/964,333, filed 4 November 1997

Title: Systems and methods for secure transaction
management and electronic rights protection

Assignee: InterTrust Technologies Corp.

Accorded Benefit: Application 08/388,107, filed 13 February 1995

Attorneys: See last page

Address: See last page

Patent: 6,138,119, granted 24 October 2000, based on application 09/300,778, filed 27 April 1999

Title: Techniques for defining, using and manipulating rights management data structures

Assignee: InterTrust Technologies Corp.

Accorded Benefit: 5,920,861, granted 6 July 1999, based on application 08/805,804, 25 February 1997

Attorneys: See last page

Address: See last page

Patent: 6,253,193, granted 26 June 2001, based on Application 09/208,017, filed 9 December 1998

Title: Systems and methods for the secure transaction management and electronic rights protection

Assignee: InterTrust Technologies Corp.

Accorded Benefit: 5,982,891, granted 9 November 1999, based on application 08/964,333, filed 4 November 1997; Application 08/388,107, filed 13 February 1995

Attorneys: See last page

Address: See last page

Senior Party

Named inventor: GREG BENSON, Dalby, Sweden
GREGORY H. URICH, Lund, Sweden
CHRISTOPHER L. KNAUFT, San Diego, CA

Application: 09/164,606, filed 1 October 1998

Title: Method and system for managing a data object
so as to comply with predetermined conditions
for usage

Assignee: Macrovision Corporation

Accorded Benefit: Patent 5,845,281, granted 1 December 1998, based
on application 08/594,811, filed 31 January 1996;
Swedish Application 9500355-4, filed 1 February 1995

Attorneys: See last page

Address: See last page

Application: 09/321,386, filed 27 May 1999

Title: Method and system for managing a data object
so as to comply with predetermined conditions
for usage

Assignee: Macrovision Corporation

Accorded Benefit: Patent 5,845,281, granted 1 December 1998, based
on application 08/594,811, filed 31 January 1996;
Application 09/164,606, filed 1 October 1998;
Swedish Application 9500355-4, filed 1 February 1995

Attorneys: See last page

Address: See last page

Part F. Count and claims of the parties

Count 1

Claim 48 of Benson's Application 09/321,386 (Benson III)

The claims of the parties corresponding to Count 1 are:

Ginter's Patent No. 5,920,861 (Ginter I):	Claims 1-4, 11-13, 34-38, 40-43, 56, 63, 64, 67 and 68
Ginter's Patent No. 5,982,891 (Ginter II):	Claims 26-31
Ginter's Patent No. 6,138,119 (Ginter III):	Claims 1-28, 30-32, 34-42, 51, 53-57 and 59-63
Ginter's Patent No. 6,253,193 (Ginter IV):	Claims 1-18 and 64-72
Benson's Application 09/164,606 (Benson II):	Claims 30-32, 34-41, 44-46, 48, 51, 56, 58-66, 68 and 69
Benson's Application 09/321,386 (Benson III):	Claims 1-3, 5-12, 15-17, 19, 22, 27, 29-37 and 39-53

The claims of the parties not corresponding to Count 1 are:

Ginter's Patent No. 5,920,861 (Ginter I):	Claims 5-10, 14-33, 39, 44-55, 59-62, 65, 66, 69 and 70
Ginter's Patent No. 5,982,891 (Ginter II):	Claims 1-25 and 32-102
Ginter's Patent No. 6,138,119 (Ginter III):	Claims 29, 33, 43-50, 52, 58 and 64
Ginter's Patent No. 6,253,193 (Ginter IV):	Claims 19-63
Benson's Application 09/164,606 (Benson II):	Claims 33, 42, 43, 47, 49, 50, 52-55, 57 and 67
Benson's Application 09/321, 386 (Benson III):	Claims 4, 13, 14, 18, 20, 21, 23-26, 28 and 38

Part G. Heading to be used on papers

The following heading shall be used on papers filed in the interference. See **STANDING ORDER ¶ 3.5.**

Filed on behalf of [name of party] Paper ¹
By: Name of lead counsel
Name of backup counsel
Street address
City, State, and Zip-Code
Tel:
Fax:

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES
(Administrative Patent Judge Jameson Lee)

KARL L. GINTER, VICTOR H. SHEAR,
FRANCES J. SPAHN and DAVID M. VAN WIE,
Junior Party,
(Patents 5,920,861; 5,982,891; 6,138,119 and 6,253,193),

v.

GREG BENSON, GREGORY H. URICH
and CHRISTOPHER L. KNAUFT,
Senior Party,
(Applications 09/164,606 and 09/321,386).

Patent Interference No. 105,193

TITLE OF PAPER

¹ Leave a blank line because the board assigns the paper number.

Part H. Summary of dates for taking action

Times for taking action are set out in the following sections of the STANDING ORDER:

- ¶ 4: date for identifying lead and backup counsel.
- ¶ 5: date for identifying any real party in interest.
- ¶ 6: date for requesting copies of involved and benefit applications and patents.
- ¶ 7: date for accomplishing certain discovery.
- ¶ 8: date for filing clean copy of claims.
- ¶ 9: date for filing clean copy of claims in cases with drawings or claims containing a means plus function limitation.
- ¶ 10: date for filing list of proposed preliminary motions.
- ¶ 13.10.2: dates for filing oppositions to Rule 635 miscellaneous motions and dates for filing replies to oppositions.
- ¶ 14.1.1: date for objecting to admissibility of evidence.
- ¶ 14.2: date for serving supplemental affidavits or evidence to respond to objection to admissibility of evidence.
- ¶ 14.3: dates when cross-examination can take place.
- ¶ 15.2: dates for taking action with respect to settlement discussions.

Part I. Order form for requesting file copies

FILE COPY REQUEST
Interference 105,193

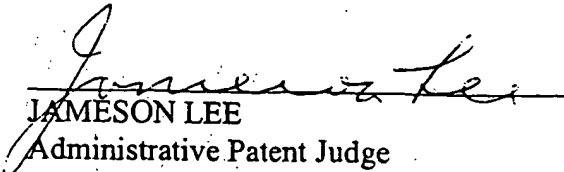
A copy of Part E of this NOTICE DECLARING INTERFERENCE should be attached to this FILE COPY REQUEST, with a circle by hand around the patents and applications for which a copy of a file wrapper is desired.

To facilitate processing of this FILE COPY REQUEST, the following information should be included:

1. Charge fees to USPTO Deposit Account No. _____
2. Complete address, including street, city, state, ZIP code and telephone number (do not list a Post Office box because file copies are sent via commercial overnight courier).

Telephone, including area code: _____

Part J. Signature of administrative patent judge


JAMESON LEE
Administrative Patent Judge

Date: 12/18/03

Enc:

Copy of STANDING ORDER

Copy of order used for setting times for taking action in the preliminary motion phase of the interference

Copy of order used for setting times for taking action in the testimony and briefing phases of the interference

Revised May 2003

cc (via Federal Express):

Attorney for GINTER:

Linda J. Thayer, Esq.
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
700 Hansen Way
Palo Alto, CA 94304

Attorney for BENSON:

Charles L. Gholz, Esq.
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.
1940 Duke Street
Alexandria, VA 22314